<<Insert logo of
Technology Provider>>

Service Level Agreement

between

EGI.eu

and

TP_LONG_NAME

1 COPYRIGHT NOTICE

2 PARTIES

This Service Level Agreement defines which services and to which level the Technology Provider commits to deliver to EGI.eu as the consumer of the services. For the remainder of this document this Service Level Agreement will be referred to as "the Agreement".

2.1 EGI.eu

To support science and innovation, a lasting operational model for e-Infrastructure is needed – both for coordinating the infrastructure and for delivering integrated services that cross national borders. The objective of EGI.eu (a foundation established under Dutch law) is to create and maintain a pan-European Grid Infrastructure in collaboration with National Grid Initiatives (NGIs) and EIROs in order to guarantee the long-term availability of a generic e-infrastructure for all European research communities and their international collaborators.

Stichting European Grid Infrastructure (EGI.eu)
P.O. Box 41882
1009 DB Amsterdam
The Netherlands

For the remainder of this document EGI.eu will be referred to as "EGI".

2.2 Service provider

<<Short text summarising the Technology Provider>>

TP_LONG_NAME
<<Address in provider's Locale format>>

For the remainder of this document the service provider will be referred to as "the Provider".

3 GOVERNANCE

3.1 Terms

The Agreement shall be binding if and only if the representatives of both the Provider and EGI have signed the Agreement.

The Agreement shall have the following date of enforcement:

<<dd. MM. yyyy>> 00:00:00 GMT

The Agreement will terminate at the following date:

<<dd. MM. yyyy>> 23:59:59 GMT

The Agreement will not terminate at a pre-defined date. A termination date may be defined at a review of the Agreement<<Delete appropriate section >>

3.2 Reviews

The Agreement may be regularly reviewed. Any part of the Agreement may be subject to review and change given that it is recorded in review minutes and a new revision of the Agreement is produced.

A review may take place any date and time agreed between the Provider and EGI. However, the Agreement shall be reviewed a minimum of once per year. In lieu of a review in any period, this Agreement shall remain in effect.

Any number of participants of either party may attend and are automatically accepted as soon as the review meeting is called to commence without objection. An agreed review date may only be cancelled with mutual agreement on a new date.

The review begins with appointing a minute taker, and ends with an agreement on the date of the next review meeting. The Provider and EGI may agree to not define a date of the next meeting.

Upon completion of the review a new version of the Agreement document is produced reflecting the changes agreed upon in the review meeting. Together with the recorded minutes this new version shall be circulated no later than 5 working days after the review meeting took place.

4 SCOPE OF THE AGREEMENT

The Provider agrees to deliver software components to EGI that, in total, implement the functionality of one or more capabilities defined in the UMD Roadmap [R 3]. The Provider agrees to indiscriminately apply the service levels defined herein to all software components delivered to EGI that are part of any version of UMD that EGI supports according to the UMD support plans.

4.1 Management & Coordination

The Provider agrees to appoint fully authorised representatives and deputies to the relevant management boards of EGI. The deputy temporarily takes over attendance, contribution and voting rights in the denominated boards at times of unavailability of the representative.

4.2 Software component delivery

4.2.1 Component roadmap and release plan

The Provider will publish a roadmap for each component it wishes to release to EGI. The roadmap may be consolidated into one document with the roadmaps for other components if the Provider releases more than one component to EGI. The roadmap must contain:

- All planned major component releases
- All planned minor component releases
- Planned new features in the component
- Any incompatibilities between releases

Incompatibilities in this context describe any change in functionality, interfaces, standards, data formats, etc. introduced in a new release, which break backwards compatibility with a previously released version of the same component, or with an existing and released version of a different component in the EGI production infrastructure.

The Provider will update the roadmap(s) every half year (six calendar months) at least one calendar month before EGI publishes the UMD Roadmap on its scheduled dates [R 1].

The Provider will make available a release plan for each component published in the Provider's software repository. The Provider may consolidate release plans of more than one component into a consolidated series of one or more documents, for a better overview. The release plan must provide the planned release dates for all maintained software components for at least one year into the future and must include the release dates for

- All major releases
- All minor releases

The Technology Provider agrees to inform EGI whenever the release plan is changed.

4.2.2 Release delivery and format

The Provider agrees to deliver releases on a regular basis and provides electronic access to the release contents as described in [R 8]. The new release must be delivered by creating a tracker artefact in GGUS containing XML based technical description of the release [R 8].

4.3 Quality Assurance

The Provider understands and accepts the Software Provisioning Process as described in [R 7] and its designated successors.

4.3.1 Acceptance Criteria

The evolution of acceptance criteria is a normal process considering the settings within which EGI and the Provider operate.

Through active participation in the TCB the Provider advises EGI on the effort required to implement any changes to generic or specific acceptance criteria that may affect any of the maintained software components that are part of, or considered to be part of, the UMD.

4.3.2 Test plans

The Provider agrees to formally provide or make available to EGI the complete test plans and results of continuous testing and integration of each maintained software component.

The test plan for a given release of one particular component must include:

- All tests available, or at least an executive overview of all tests available
- The complete, detailed list of all tests executed for the given release of the component in question
- The complete, detailed result of each executed test
- References to descriptions of, and any required 3rd party software packages necessary to execute the supplied test plans.

The test plans as described above must be made available to EGI prior to the planned release date for review:

- Major release: At least 20 working days
- Minor release: At least 15 working days
- Revision release: At least 10 working days
- Emergency release: N/A

Prior to entering EGI's Software Provisioning Process [R 7] and upon request of EGI's appropriate management unit, the Provider, in collaboration with EGI, agrees to the best of their ability to:

- Rerun the complete test plan for major releases
- Run a subset of the tests of the test plan (chosen by EGI) for minor releases

4.4 Issue management

The Provider has appointed personnel for technical issues concerning the maintained software components. Those technical contacts must be fully authorised to act as the Provider's representative in collaboration with EGI DMSU [R 6] regarding the triaging, assessment and resolution of any technical issues concerning the software components developed and maintained by the Provider.

4.4.1 Issue management infrastructure

EGI uses GGUS for 2nd level (DMSU) support. For 3rd-level support, EGI provides the Technology Provider with a provider-specific Support Unit (SU) in GGUS as 3rd level support interface. Monitoring and reporting of provider performance is implemented through this SU.

4.4.2 Issue Resolution

The Provider constructively works in close collaboration with EGI DMSU on jointly investigating issues raised against software components maintained by the Provider. The investigation includes triaging the issue or incident, the problem and any known impacts. The details of the process of collaboration with the DMSU are outlined in [R 6].

In case the triage resolves to the production of a new release of the affected software component DMSU and the service provider jointly agree on an Estimated Time of Availability (ETA) of the necessary new release of that software component.

The Provider agrees to prioritise the effort to resolve and fix reported issues according to their priority as set in GGUS, in the following order, while respecting the constraint of the agreed ETA:

1. Top priority
2. Very urgent
3. Urgent
4. Less Urgent

4.5 Vulnerability management

The Provider has appointed personnel for vulnerability issues concerning the maintained software components. Those security contacts must be fully authorised to act as the Provider's representative in collaboration with EGI SVG [R 9] and related boards regarding the triaging, assessment and resolution of any vulnerability issues concerning the software components developed and maintained by the Provider.

Any appointed security contact for any delivered software component must respond to any request by the EGI SVG and associated groups (e.g. RAT). The response must be as soon as possible, or at least within 2 working days.

4.5.1 Vulnerability Resolution

The Provider agrees that any software vulnerability found in their delivered software while running on EGI production infrastructure must be handled using the SVG process [R 5].

The Provider agrees that any software vulnerability in their delivered software found outside of this process must be reported to the EGI SVG. If the vulnerability is reported before a fix is available, the vulnerability must be treated and resolved as if found on EGI production infrastructure, i.e. it must be handled using the SVG process. If the vulnerability is reported after a fix is available, the Provider coordinates with SVG to make available the new release including an appropriate advisory for SW release on EGI production infrastructure.

The Provider agrees to prioritise vulnerability resolution according to their risk assessment, in the following order:

1. Critical
2. High
3. Moderate
4. Low

For any vulnerability found in any software component delivered by the Provider, the Provider agrees to the best of their ability that no information about the vulnerability shall be disclosed to the public without consent of the SVG. Other Software Vulnerability groups may be informed without prior consent of the EGI SVG, provided they have a non-disclosure policy, which is compatible with that of the EGI SVG. Also, IGE and any other vulnerability groups informed must ensure that a fix is available in the UMD prior to public or other widespread disclosure of the vulnerability.

4.6 Service Requests

Integral part of supporting the services outlined in the Agreement the Provider will respond to Service-related incidents and/or requests submitted by EGI or one of the authorised GGUS 2nd level support units within the following time frames:

GGUS ticket priority	Response time	Comments
Top Priority	4 hours	During EGI office hours, see below.
Very urgent	2 working days	In the respective time zone of the service provider's mailing address as given in section 2.2
Urgent	5 working days	
Less urgent	15 working days	

Working day

A working day is defined as a normalised day of 8 business hours from 9:00 to 17:00 o'clock, on five days a week from Monday to Friday.

5 PERFORMANCE MEASUREMENT

The performance of the Provider shall be monitored against the metrics and objectives described in this section. The metrics and objectives defined in this section are scoped per Provider and are standing agenda items of each Agreement review conducted.

5.1 Definition of terms

TD – Target Date

The Target Date is set by the EGI SVG according to the Risk Category after the vulnerability has been assessed by the EGI SVG Risk Assessment Team. Vulnerabilities found to be valid are placed in 1 of 4 risk categories: 'Critical', 'High', 'Moderate', or 'Low' Risk. A fixed target date is set for each of these categories to 3 working days, 6 weeks, 4 months or 1 year for Critical, High, Moderate or Low vulnerabilities, respectively.

ETA – Estimated Time of Availability

The ETA is the agreed date of availability to EGI of a release of a software component that fixes one or more reported issues. The ETA may be revised between DMSU and the Provider.

5.2 Metrics

Each metric is a positive integer number, including 0 (zero). “Secondary” metrics (i.e. metrics with an ID counter larger than 1) are constrained in that they cannot reach numbers greater than the pertinent “main” metrics (i.e. M.*.1).

All metrics are collected on a monthly basis, starting on the first calendar day of the month, and ending on the respective last day of the month.

Metric ID	Metric	Explanation
M.SVG.1	Number of confirmed new vulnerabilities per month	The total number of vulnerabilities discovered in all maintained software components, whether within EGI activities or outside, are collected and published. Aggregated during the reporting month.
M.SVG.2	Number of fixes delivered within TD	All fixes that are delivered within TD *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.SVG.3	Number of fixes delivered after TD	All fixes that are delivered *after* TD *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.SVG.4	Number of confirmed open vulnerabilities which have exceeded the TD	Number of confirmed vulnerabilities, which have not been fixed and have passed the TD at the time of calculating. Current value taken at the end of the reporting month on the last working at 18:00 CE(S)T.

M.SVG.5	Total number of open vulnerabilities	Current value taken at the end of the reporting month on the last working day at 18:00 CE(S)T.
M.SVG.6	Number of requests to the Provider	The total number of requests for information and/or participation in investigation of issues to IGE concerning vulnerabilities. Aggregated during the reporting month.
M.SVG.7	Number of contact responses below 2 day target	Each request made by the SVG or associated boards that were not reacted upon within 2 working days are counted. Aggregated during the reporting month.
M.DMSU.1	Number of issues assigned to the Provider	The total numbers of confirmed issues that require the Provider's effort to produce a new release are counted. Aggregated during the reporting month.
M.DMSU.2	Number of issues with revised ETA	The total number of issues for which the Provider changed the ETA are counted. Aggregated during the reporting month.
M.DMSU.3	Number of fixes delivered within ETA	All fixes that are delivered within ETA *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.DMSU.4	Number of fixes delivered within ETA + 1 week	All fixes that are delivered within ETA + 1 calendar week *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.DMSU.5	Number of fixes delivered within ETA + 1 month	All fixes that are delivered within ETA (+ 1 calendar month) *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.REPO.1	Number of releases delivered to EGI	The total number of releases made available to EGI through the SW Rollout process is counted. Aggregated during the reporting month.
M.REPO.2	Number of releases that passed the quality criteria verification.	All releases that passed the quality criteria verification process are counted. Release submissions that result in changes of quality criteria applicable to the pertinent component are not counted in this metric. Aggregated during the reporting month.
M.REPO.3	Number of releases that passed StageRollout verification	All releases that passed the StageRollout phase of the SW rollout process hence are accepted for production use, are counted. Aggregated during the reporting month.
M.MISC.1	Number of violations of service request response times	Every occurrence of a violation of the service request response times agreed to in section 4.6 is counted.

		Aggregated during the reporting month.
M.MISC.2	Number of releases that failed any mandatory Generic Documentation Quality Criterion	Documentation quality is a critical software quality criterion, but not part of the decision to accept or reject software based on technical failures. Aggregated during the reporting month.

5.3 Objectives

Objectives are decimal numbers with a precision of 2 decimals rounded. In case of any main metric, at the point of collection, has the value 0 (zero) the related objective shall have the value "0.00%"

Objectives are calculated using monthly metering of the metrics defined in section 5.2.

Objective ID	Objective	Calculation	Target
O.SVG.1	Proportion of issues fixed within TD	100 * M.SVG.2 / (M.SVG.2 + M.SVG.3 + M.SVG.4)	90%
O.SVG.2	Proportion of open issues beyond TD	M.SVG.4 / M.SVG.5 * 100	10%
O.SVG.3	Responsiveness of security contacts to vulnerability issues	(M.SVG.7 / M.SVG.6) * 100	100%
O.DMSU.1	Success rate of timely delivery within ETA	(M.DMSU.3 / M.DMSU.1) * 100	85%
O.DMSU.2	Success rate of timely delivery within ETA + 1 week	(M.DMSU.4 / M.DMSU.1) * 100	10%
O.DMSU.3	Success rate of timely delivery within ETA + 1 month	(M.DMSU.5 / M.DMSU.1) * 100	5%
O.REPO.1	Formal quality of component releases	(M.REPO.2 / M.REPO.1) * 100	90%
O.REPO.2	Functional quality of component releases	(M.REPO.3 / M.REPO.1) * 100	90%
O.MISC.1	Service response time violation	M.MISC.1	0
O.MISC.2	Documentation quality failure	M.MISC.2	0

Due to the expected small number of software Products contributed by IGE a sensible relation-based metering of objective targets is not possible. Instead, IGE and EGI agree that objectives undergo quarterly review collecting input across EGI management bodies and activities (SVG, RAT, DMSU, TCB, etc.) and a formal overall ratification that collected metrics are within reason.

The performance of IGE in said activities will be individually reviewed and assessed on the following scale:

1. Performance above expectations
2. Performance as expected
3. Performance below expectation

The review will include assessment of the past period, and expectations for the subsequent period.

<<Remove the highlighted section for Technology Providers that deliver a large amount of software into the EGI – use this to negotiate a performance review for Technology Providers that deliver small amounts of software to avoid large oscillations in the collected metric data, potentially missing objectives just because of occasionally appearing software incidences.>>

6 PROBLEM MANAGEMENT & REMEDY

6.1.1 Agreement provisioning

Any failures during the provisioning of the Agreement itself must be reported to the EGI CTO (cto@egi.eu) and the Provider's contact person appointed for provisioning the Agreement.

Likewise, any perceived failure of the SLA document itself must be reported to the parties signing this Agreement.

6.1.2 Escalation

EGI and the Provider agree in a practical and benevolent approach in resolving any disputes or disagreements over any operational aspect of this agreement, or any process included herein or referenced externally.

Any reasonable and feasible attempt should be undertaken to resolve disagreements and disputes in the relevant activities on the operational day-to-day level (e.g. DMSU, RAT).

Issues that remain unresolved shall be brought to the attention of the TCB within reasonable time. The TCB shall then attempt to resolve the issue through common communication means as described in the TCB Terms of Reference [R 4]. Any issue discussed at the TCB will be handled openly and indiscriminately.

Further escalation if required, must be directed to the EGI Director and appointed overall managerial contact of the Provider.

If a resolution and consensus cannot be reached at this level, escalation may be directed to the EGI Executive Board. The EGI EB is the last instance that may reach a resolution to an escalated dispute. In case negotiations at this level fail to produce a resolution to the dispute, either party of this Agreement may initiate an extraordinarily, yet orderly, termination of the agreement and Memorandum of Understanding of the signed parties. The process of an orderly termination of the agreement is defined in section 8.

7 EGI DUTIES

To support the Provider in fulfilling the duties described in section 4, EGI agrees to the following.

EGI will communicate requirements and use cases collected from its end user and operations communities to the Provider through the Technology Coordination Board. These prioritised requirements may span new or existing features related to the maintained software components, and are communicated publicly and indiscriminately to any technology provider partaking in the TCB.

EGI will define and publish the environment (or environments) that the maintained software components are required to work in.

EGI will provide generic acceptance criteria related to all software components contributed to EGI.

EGI will provide specific acceptance criteria related to all software components maintained by the Provider.

EGI will inform the Provider of issues reported to EGI related to the maintained software components in use on EGI's production infrastructure.

EGI will include the Provider in the triaging of the issues mentioned above through the appointed DMSU.

EGI will provide access to boards, process and knowledge of EGI's SVG to the Provider in order to develop and contribute corrections necessary to the maintained software components.

EGI will provide contact points for issue management, vulnerability management and general roadmap and requirements issues. The respective personnel will respond within 2 working days to issues raised by the Provider.

8 TERMINATION AND RELEASE FROM AGREEMENT

The Agreement may terminate at a date defined at the Agreement's inception (see section 3.1) or at a date agreed upon in a review. In some circumstances the Agreement may terminate because of breach of the Agreement.

Under all circumstances the termination of the Agreement must maintain productivity of EGI infrastructure at all times.

Upon termination of the Agreement, the Provider is liberated from the obligation to provide any update on roadmaps, test plans or new releases to the agreed list of software components, except for already existing, confirmed issues and vulnerabilities reported against maintained software components.

Upon termination of the Agreement EGI retains the right to operate the software components under the auspices of this Agreement at the current version running in the production infrastructure. To ensure continuous availability EGI may decide to roll back any delivered software component to a version EGI deems stable and suitable for production use on its infrastructure.

Upon termination of the Agreement EGI and the Provider agree to phase out any software component specified in this Agreement according to EGI's procedures for Software Lifecycle Management in case an alternative complete implementation of the respective UMD capability is available to EGI.

8.1 Conditions of premature Agreement termination

EGI retains the right to terminate the Agreement whenever any of the following events occurs:

- The Provider persistently fails to meet the service levels defined in section 5.3. Persistent failure is defined as not meeting the defined objective targets for 3 consecutive metering periods as defined in section 5.
- The Provider persistently fails to contribute to the TCB of EGI. Failure to contribute includes representatives not joining F2F meetings or conference calls, and no contribution towards determining a Target Date for Vulnerability fixes or Estimated Times of Availability for bug fixes, respectively. Persistent failure is defined as missing the attendance and contribution levels defined for the respective body.

9 REFERENCES

The following table lists all references made throughout the Agreement. EGI agrees to make available to the Provider copies of any referenced document listed herein.

R 1	EGI-InSPIRE Description of Work, Part A, WT3, Work package 5, https://documents.egi.eu/document/10
R 2	EGI Technology Roadmap, To be published
R 3	D5.2 UMD Roadmap, https://documents.egi.eu/document/272
R 4	Technology Coordination Board Terms of Reference, https://documents.egi.eu/document/109
R 5	MS405: Incident Response Procedure & The software vulnerability issue handling process: https://documents.egi.eu/document/47
R 6	MS507: DMSU Operations Procedures, https://documents.egi.eu/document/504
R 7	MS508: Software Provisioning Process https://documents.egi.eu/document/505
R 8	MS506: EGI Software Repository Architecture and Plans https://documents.egi.eu/document/503
R 9	Software Vulnerability Group Terms of Reference https://documents.egi.eu/document/108

Service Level Agreement between EGI.eu and TP_SHORT_NAME

IN WITNESS WHEREOF, the Parties have caused their duly authorised representatives to sign two originals of this Service Level Agreement, in the English language.

The following agree to the terms and conditions of this SLA:

_____	_____
Dr. Steven Newhouse	**SIGNER_NAME**
Director, EGI.eu	**SIGNER_FUNCTION, TP_SHORT_NAME**
_____	_____
Date	**Date**